“Intrusion Detection System: stato dell'arte e ricerca”

Valerio 'click' Genovese <click@spine-group.org>
Marco 'embyte' Balduzzi <embyte@spine-group.org>

Cos'è un Intrusion Detection System (IDS)?

- *"Intrusion detection systems analize information about the activity performed in a computer system or network, looking for evidence of malicous behavior" [1]*

- Ovveso, un IDS è un sistema che rileva accessi non consentiti o potenziali attacchi a un sistema informatico per mezzo di sorgenti d'informazioni disponibili sul sistema (log) o dalla rete (traffico di rete).

- Una intrusione è un tentativo di accesso deliberato e non consentito a un sistema informatico con il fine di violare informazioni riservate o impedirne il funzionamento (DoS).

[1] James. P. Anderson. Computer Security Thread Monitoring and Surveillance, April 1980

Il Puzzle

- Un IDS non si sostituisce ai normai controlli.
- Un IDS deve essere affiancato da altri meccanismi di sicurezza
- Sono un campanello d'allarme e non fermano l'attacco. Esistono sistemi apposta che fan questo (vedi IPS poi..)

Perchè aver bisogno di un IDS?

- Diventano maggiormente necessari man mano che il rischio associato alla perdita di informazioni riservate o alla impossibilità di offrire un servizio informatico gravano sulla funzionalità della ditta.

- Aumento degli attacchi informatici
  - Connessioni a banda larga (ADSL) disponibili a basso costo
  - Aumento del numero di script-kiddie (internet disponibile a basso costo a tutti)
  - Maggior diffusione di worms e virus per mezzo di email
  - Spyware nei software P2P

- Alcuni esempi:
  - Dos contro Yahoo e Ebay
  - Codered

SANS Windows Top 10 Vulnerability

- Top Vulnerabilities to Windows Systems

W1 Internet Information Services (IIS)
W2 Microsoft SQL Server (MSSQL)
W3 Windows Authentication
W4 Internet Explorer (IE)
W5 Windows Remote Access Services
W6 Microsoft Data Access Components (MDAC)
W7 Windows Scripting Host (WSH)
W8 Microsoft Outlook and Outlook Express
W9 Windows Peer to Peer File Sharing (P2P)
W10 Simple Network Management Protocol (SNMP)

SANS Unix Top 10 Vulnerability

- Top Vulnerabilities to UNIX Systems

U1 BIND Domain Name System
U2 Remote Procedure Calls (RPC)
U3 Apache Web Server
U4 General UNIX Authentication Accounts with No Passwords or Weak Passwords
U5 Clear Text Services
U6 Sendmail
U7 Simple Network Management Protocol (SNMP)
U8 Secure Shell (SSH)
U9 Misconfiguration of Enterprise Services NIS/NF
U10 Open Secure Sockets Layer (SSL)

Perchè non basta un Firewall?

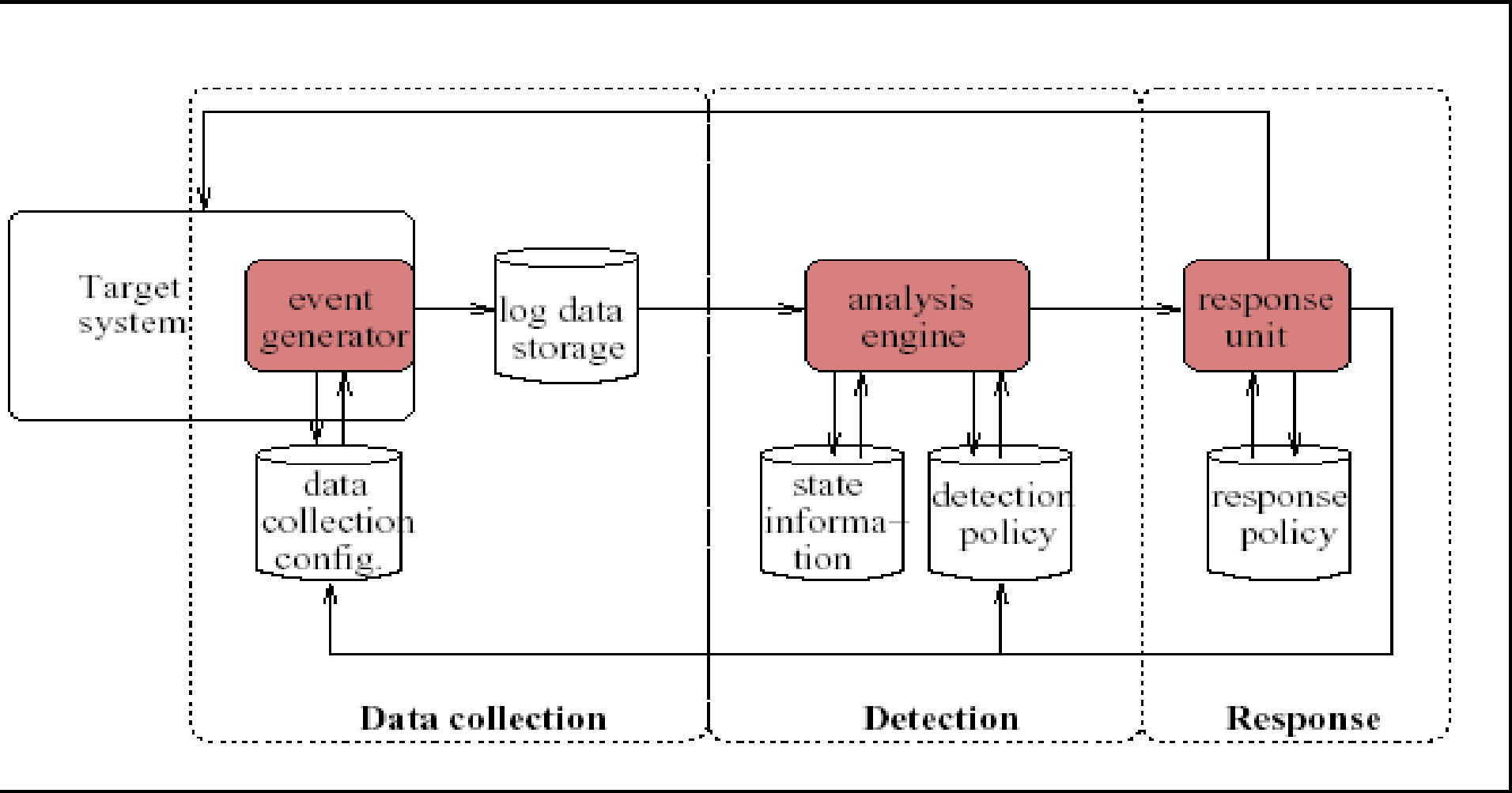
- L'appoccio e il metodo attreverso cui si vuole aumentare il livello di sicurezza in una rete sono fondamentalmente diversi tra IDS e firewall

- Il firewall e' uno strumento proattivo che,in base a oppurtune flags, regola e filtra il flusso di dati in un AS

- L'IDS si offre principalmente come una soluzione atta al monitoraggio della rete. Questo avviene attraverso una serie di regole e di algoritmi molto flessimibili atti ad individuare gli attacchi che sono rivolti al nostro AS

- Ricordiamoci sempre la il concetto di “puzzle”: tanti strumenti per “avere la situazione sotto controllo”

Architettura di un generico IDS



Vari modi di classificazione

- Differenti modi di classificare gli IDS
  - Sorgenti di Informazione (Network, Host-based)
  - Metodo di rilevamento (Misuse, Anomaly)
  - Meccanismi di analisi (Real-time, Batch/Offline)

- Tipi di attacchi rilevati dalla maggioranza degli IDSs
  - Scans/probes, Denial of Service (DoS)
  - User-To-Root (U2R), Remote-To-Local (R2L)

On-line vs. off-line

- On-line
  - generazione degli alert in base ad eventi correnti
  - alto peso computazionale
  - uso di trigger
  - esempio: network-based ids

- Off-line (batch):
  - registrazione degli eventi su log
  - analisi degli stessi periodicamente
  - risultato non istantaneo
  - possibilità di history (data mining)

Misuse vs Anomaly detection

- Misuse Detection

  L'IDS analizza le informazioni che raccoglie e le confronta con un grande database contentente le attack signatures. Essenzialmente, l'IDS cerca uno specifico attacco che e' stato gia' documentato.Come in un virus detection system, la qualita' di un misuse detection software dipende solamente dall'affidabilita' del database che utilizza per il confronto.

- Anomaly detection

  In anomaly detection, l'amministratore di sistema definise alcune lineeguida, come peresempio lo stato della traffico di rete, i protocolli, la grandezza dei pacchetti e quant'altro. L'anomaly detector controlla segmenti di rete per confrontare il loro stato con le normali lineeguida e controlla eventuali anomalie.

Misuse vs Anomaly detection

- Misuse Detection (pro/contro)
  - ✓ *Appoggiarsi ad un grande database puo' essere certamente una valida soluzione per rilevare gli attacchi noti*
  - ✓ *Il lavoro dell'amministratore sotto questo punto di vista e' facilitato dal momento che non e' lui a definire le linee guida*
  - ✗ *Non sempre gli attacchi corrispondono a signatures ben definite su database, in un certo senso l'attaccante e' potenzialmente sempre in vantaggio rispetto all'ammnistratore dal momento che puo' usufruire di attacchi "nuovi" o comunque non standard*
  - ✗ *Stretta dipendenza dal database*

- *Anomaly detection*
  - ✓ *E' sicuramente una soluzione piu' flessibile e potenzialmente piu' promettente.*
  - ✓ *Definire delle lineeguida generali puo' essere utile per prevenire...*

Misuse vs Anomaly detection

... anche attacchi nuovi non salvati sui database utlizzati dai misuse

✓ Non dipende dal database e' quindi puo' essere configurato ad-hoc per la rete e per le funzioni che essa deve svolgere

✗ Non sempre le lineeguida possono rivelarsi utili, se settate in maniera troppo generale si avra' una generazione eccessiva di falsi positivi.

✗ Maggiore carico di lavoro in mano all'amministratore

Host Intrusion Detection Systems

- Analisi in real-time delle attivita'
  - Check dei log
  - Analisi delle applicazioni
  - Controlli a livello kernel tramite moduli
  - Monitoring degli user
  - Scrittura degli alert sui log

- In alcuni casi e' previsto un intervento “attivo” con il bloccaggi di alcune attivita'

- O.S. Dependent

- Check sullo stream del solo host

Network Intrusion Detection Systems

- Utilizzo dei sensori tramite sniffing del traffico
- Configurazione dei sensori attraverso un set di regole basate sulla trassonomia degli attacchi
- Segnalazione della anomalie e eventuali interventi automatici
- Posizionamento dei sensori nei nodi ad alto traffico della rete
- Panoramica molto piu' unitaria dell'intera rete

IDS vs IPS

- IPS pro/contro

✔ *Modalita' di “intervento” attiva in rapporto a quella di un IDS secondo l'applicazione di opportuni algoritmi*
✔ *“Collaborazione” tra firewall e IDS coordinate appunto dall'IPS*
✔ *Più appetibili dal punto di vista commerciale “ormai quasi tutti i vendor propongono IPS”*

✘ *Intervenire automticamente non sempre puo' essere una valida soluzione*
✘ *In caso di falsi positivi doppio fallimento*
✘ *Alta generazione di traffico*

Snort-line IPS

- Da http://snort-inline.sourceforge.net/ : *“Snort_inline is basically a modified version of Snort that accepts packets from iptables, via libipq, instead of libpcap. It then uses new rule types (drop, sdrop, reject) to tell iptables whether the packet should be dropped, rejected, modified, or allowed to pass based on a snort rule set. Think of this as an Intrusion Prevention System (IPS) that uses existing Intrusion Detection System (IDS) signatures to make decisions on packets that traverse snort_inline”.*

- Esempio pratico di “collaborazione” tra IDS e firewall, integrati poi insieme a livello logico

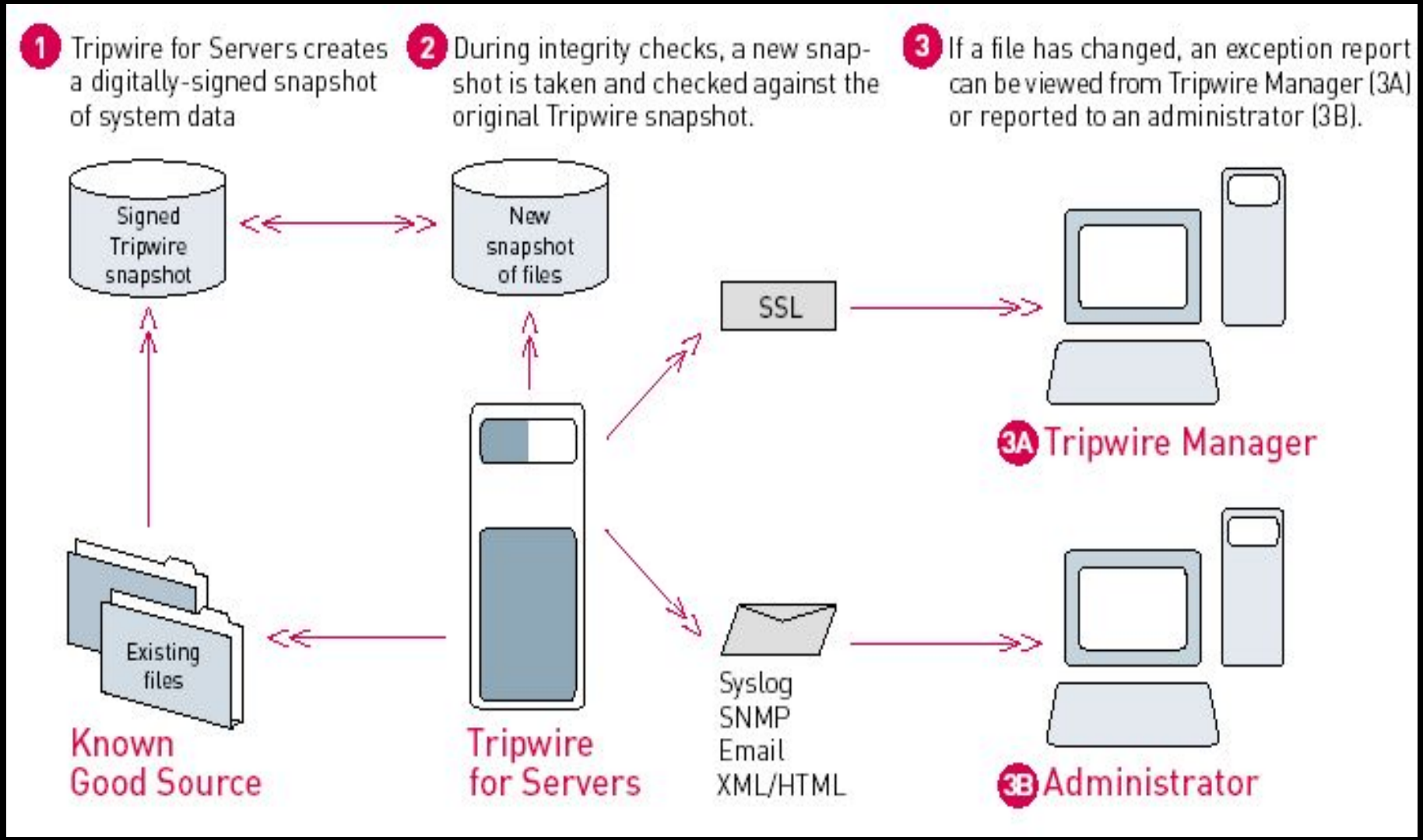
Host-Based IDS

- Filesystem monitoring HIDS: controllo sul filesystem (MD5, timestamp, dimesione) per mezzo di un confronto con un DB trusted
  - TripWire (http://www.tripwire.org)
  - Aide (http://www.cs.tut.fi/~rammer/aide.html)

- Log monitoring HIDS: analisi dei log di sistema per scoprire attività illecite
  - Swatch (http://swatch.sf.net)
  - Logsurfer (http://www.cert.dfn.de/eng/logsurf/)
  - Logwatch (www.logwatch.org)

- Os monitoring: controllo delle attività base del sistema operativo per mezzo di moduli del kernel
  - grsecurity (http://www.grsecurity.net)
  - LIDS (http://www.lids.org)

Host-Based IDS - TripWire



- Caratteristiche:
  - Protezione contro i più comuni metodi per exploitare un sistema:
    - Modifica dello spazio d'indirizzamento
    - Race conditions (specialmente in /tmp)
    - Rottura di un ambiente chrottato
  - Ricco sistema di ACL con un tool di amministrazione user-space
  - Supporto per sysctl (modifica al volo via procfs)
  - Meccanismo di logging degli attacchi e auditing di alcuni eventi:
    - Exec()
    - Chdir(2)
    - mount(2)/unmount(2)
    - Creazione ed elimina di IPC (semafori, code di messaggi)
    - Fork fallite [...]
  - Supporto per l'architettura multi-processore

Network and service monitoring

- OpenSource
- Sistema di monitoring remoto degli host e dei servizi
- Gestione degli allarmi via email, instant messages e sms
- Pannello di amministazione raggiungibile via browser
- Alta estendibilità per mezzo di plug-ins
- Sito: http://www.nagios.org

Snort – The Open Source Network Intrusion Detection System

- Da http://www.snort.org: "*Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plugin architecture. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to Windows clients using Samba's smbclient.*"

Prelude IDS – Un IDS ibrido

- HIDS+NIDS=Hybrid IDS
- Da http://www.prelude-ids.org/: *"Prelude is an innovative Hybrid Intrusion Detection system designed to be very modular, distributed, rock solid and fast. The project has been initiated and is leaded by Yoann Vandoorselaere since 1998."*
- *"Prelude takes benefits from the combination of traces of malicious activity from differents sensors (snort, honeyd, nessus vulnerability scan, hogwash, samhain, systems logs, and others) in order to better qualify the attack and in the end to perform automatic correlation between the various traces."*

I limiti dei network-based IDS “classici”

- Reti switchate: dove mettere il sensore?
- Banda satura sulla porta di monitoring
  - Scenario:
    - 3 host - 40mbps di traffico ciascuno
    - 120mbps di traffico totale > 100mbps porta monitoring
    - 20% dei pacchetti persi
- Carico computazionale maggiore
- Traffico crittografato (https, ssh, VPN)

  - Mancanza di contesto
  - Alto numero di falsi positivi

- Provare per credere! IDS stressing tools
  - Stick (http://www.eurocompton.net/stick/projects8.html)
  - Sneeze (http://snort.sourceforge.net/sneeze-1.0.tar)

Cosa si intende per “mancanza di contesto”?

- Questo è un alert di un NIDS (*) relativo ad un client Back Orifice
- Macchina vittima Mrs.Howell.Opus1.COM

(*) http://www.sourcefire.com/

SOURCEfire Network Sensor SOURCEfire

EVENTS | RULES | STATUS | ADMIN | LOGOUT | Help

Packet Display

Deactivate Name Resolution | Display Session

Event Data

Message	spp_bo: Back Orifice Traffic Detected	Generator ID	105
Classification	None	Snort ID	1
Priority	0	Revision	1

Ethernet Header

SRC MAC:	00:08:21:04:16:40	DST MAC:	00:50:5A:00:23:32	Type:	0x0800

IP Header

Version:	4	Header Len:	5	TOS	0	Total Len (in bytes)	47
16-bit ID	0	Frag Flags	DF	13-bit offset		0x0000 (0)	
TTL	44			Protocol		UDP	
Source IP				216.12.210.209			
Destination IP				192.245.12.221 Mrs.Howell.Opus1.COM			

UDP Header

Source Port:	56742	Dest Port:	31337
Length:	27		

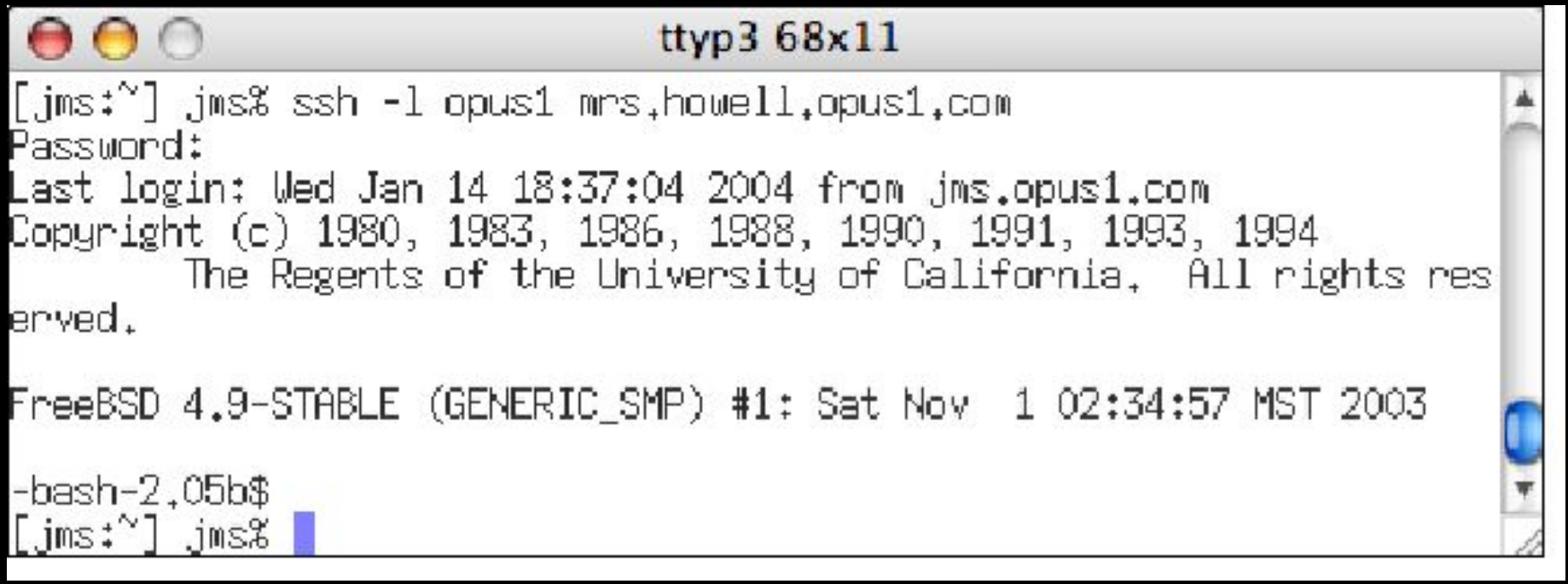
Packet Payload

Payload Length: 19 bytes

```
0x0000: CE 63 D1 D2 16 E7 13 CF 38 A5 A5 86 B2 75 4B 99          .c......8....uK.
0x0010: AA 32 58                                                 .2X
```

Cosa si intende per “mancanza di contesto”?

- Eppure non mi pare che FreeBSD sia una delle piattaforme supportate da Back Orifice!



- E' un falso positivo!

Cosa si intende per “mancanza di contesto”?

- SE l'Intrusion Detection System
  - conoscesse la *tipologia della rete* monitorata
  - conoscesse il *sistema operativo* dei sui host
  - conoscesse i *servizi* disponibili sulla macchina
  - conoscesse la *versione* di tali servizi
  - conoscesse le *vulnerabilità* sfruttabili dall'attaccante

- ALLORA avrebbe giustamente ignorato la richiesta Back Orifice

- Ron Gula (Tenable): “raw-intelligence” vs “well-qualified intelligence”

In 2000 Martin Roesch coined the “Target-Based IDS” term

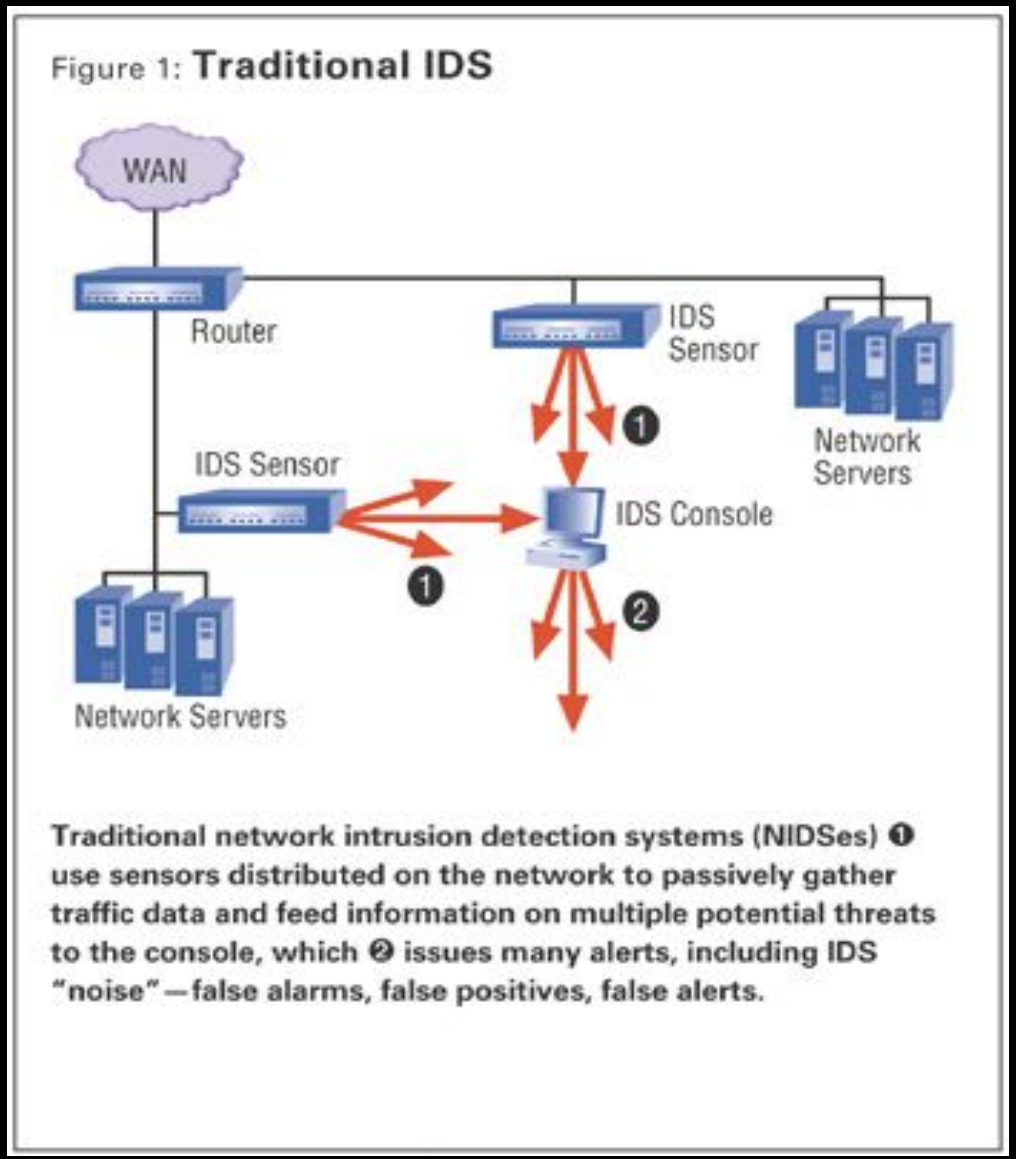
- Roesch: *“The entire value of IDS is in its output, if we can't reduce that output to information that's useful to us as administrators then the usefulness of entire system is limited.”*

- Due componenti
  - Sensore Target-Based: possiede conoscenza degli host (OS e servizi) e della topologia della rete
  - Correlatore d'eventi Target-Based: l'output del sensore è comparato con la conoscenza delle vulnerabilità

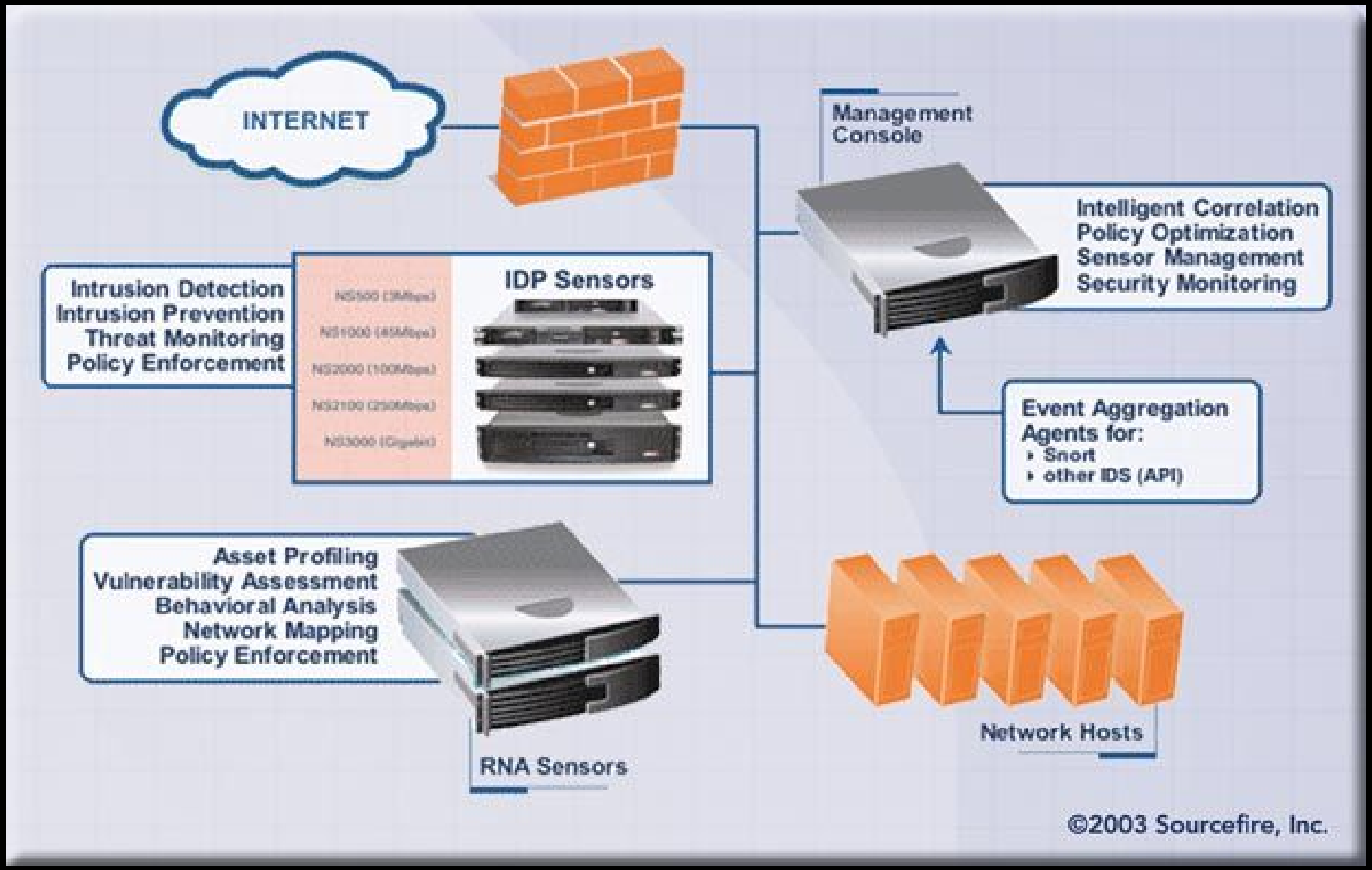
- Sourcefire: l'idea di Martin si fa realtà

Un IDS tradizionale...

- ...genera una gran quantità di allarmi che arrivano direttamente alla console d'amministrazione
- L'operatore impazzisce a controllare tutti gli allarmi quindi non riesce a individuare quelli importanti (l'ago nel pagliaio)



La risposta di Roesch



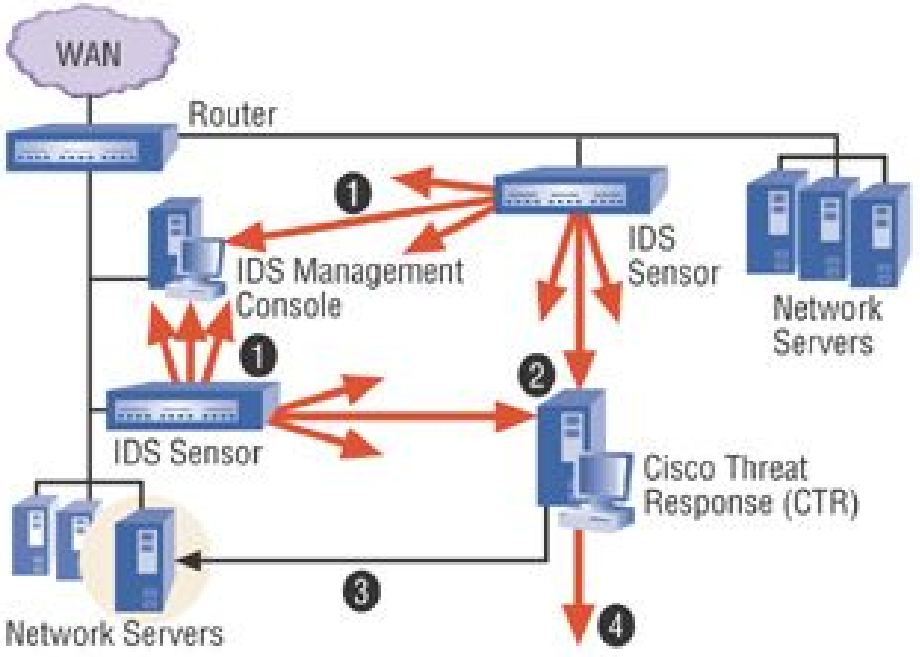
Real-Time Network Awareness

- Da http://www.sourcefire.com: *“RNA's innovative passive sensing technology constantly monitors all network assets (servers, routers, PC?s, firewalls, wireless access points, etc.) and provides a persistent view of:*
  - *Network Asset Profiles (MAC address, OS and version, services and versions, ports, etc.)*
  - *Asset Behavioral Profiles (traffic flow, traffic type, traffic volume, etc.) (release 2)*
  - *Network Profiles (hop count, TTL parameters, MTU parameters, etc.)*
  - *Security Vulnerabilities*
  - *Change Events (new assets, changed assets, behaviorally anomalous assets, etc.)”*

I concorrenti: confronto tra tre approcci - Cisco Threat Response

- Standalone product
- Scanner rete/vulnerabilità + amministrazione in un unico box
- Difficoltà di gestione in una rete molto segmentata e ampia
- Scanning attivo
- Scanning reattivo: verifica della vulnerabilità dopo l'alert
- Definizione del tempo di caching delle informazioni
- Possibilità di schedulare lo scanner rete/vulnerabilità
- Tradeoff tra traffico di rete e anzianità delle informazioni

Figure 2: **Cisco Threat Response**

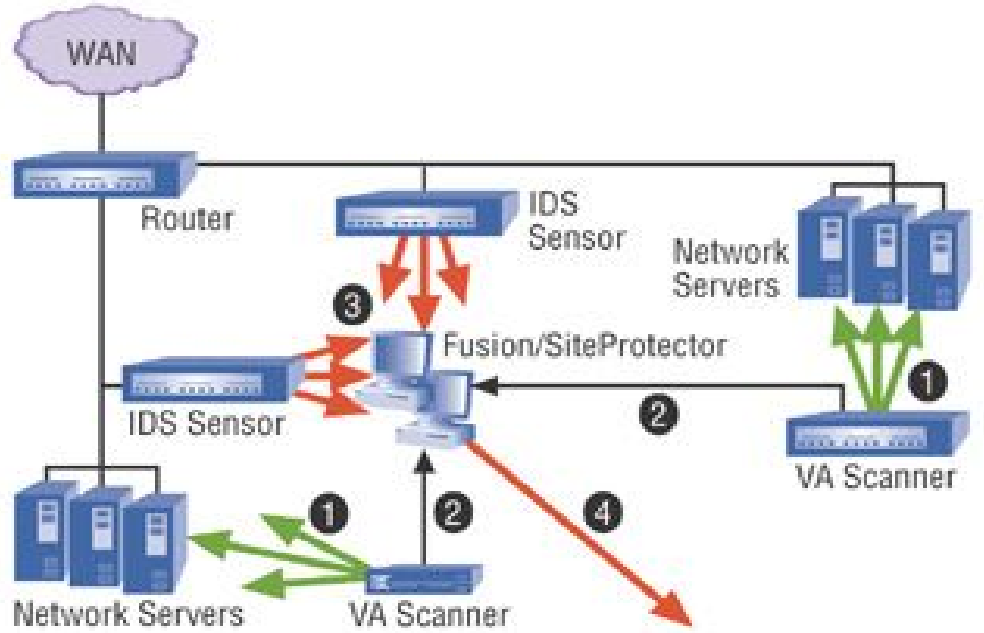


Cisco Threat Response gathers network traffic data through IDS sensors, which pass the data on multiple potential threats to both ❶ the IDS Management Console and ❷ the CTR Console, which aren't integrated. When the CTR console receives information about a potential attack, it ❸ scans the target host to determine if the attack applies. If CTR ❹ concludes there's an attack, it issues an alert. In addition, CTR can conduct active network scans with its bundled VA scanner.

I concorrenti: confronto tra tre approcci – ISS Fusion

- Toolkit
- Scanner rete/vulnerabilità + amministrazione separati
- Fortemente scalabile
- Scanning attivo
- Possibilità di schedulare l'attività del VA Scanner
- Genera alto traffico
- Attività fortemente invasiva

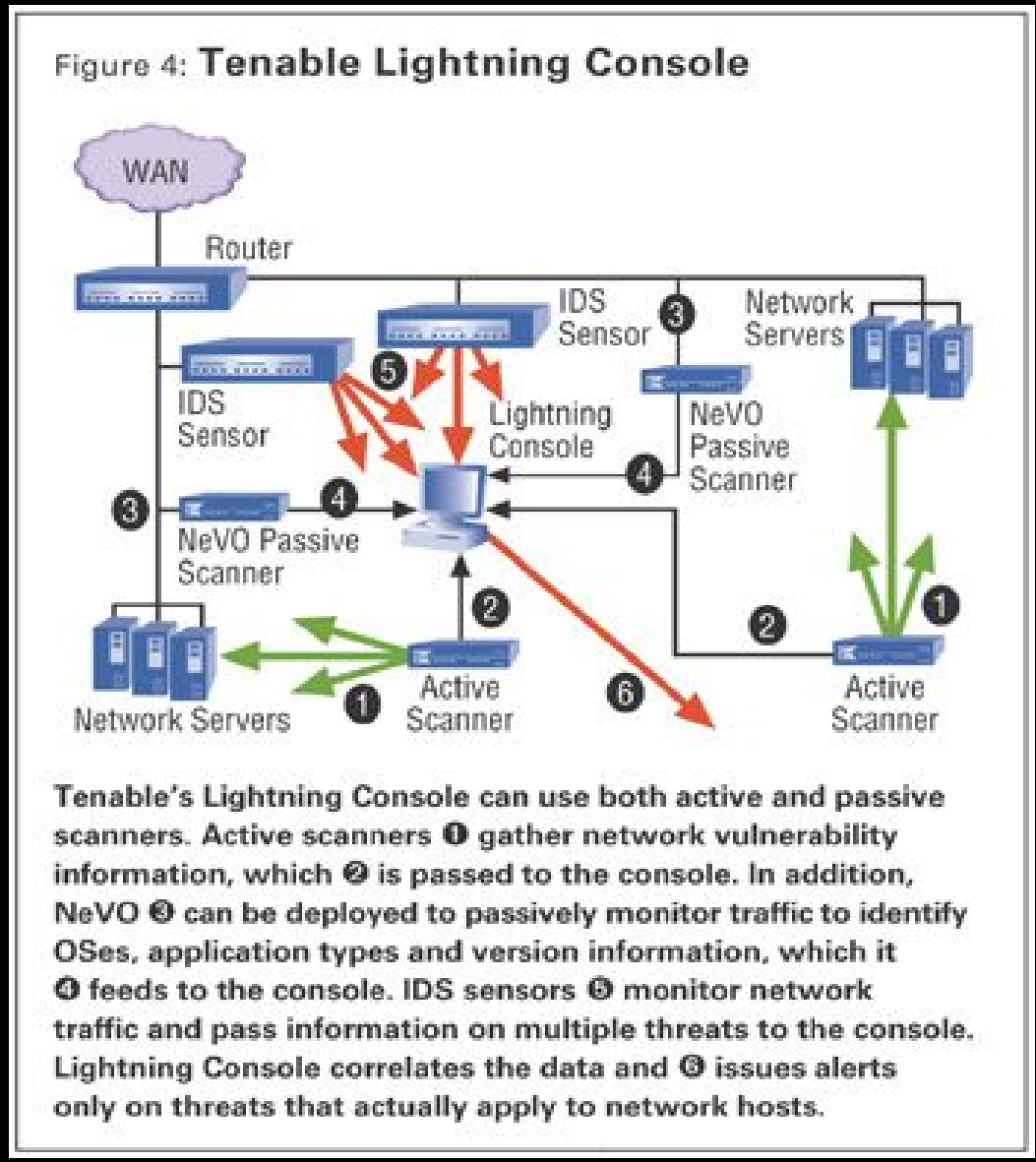
Figure 3: **Internet Security Systems Fusion**



Internet Security Systems' target-based NIDS ❶ gathers network vulnerability information through active scans, and ❷ feeds the data to the SiteProtector and Fusion consoles. IDS sensors ❸ gather traffic data, and pass information on multiple threats to the consoles. The Fusion correlation engine matches threat data against known network vulnerabilities and ❹ issues alerts only on threats thatactually apply to the network hosts.

I concorrenti: confronto tra tre approcci – Tenable Lighting Console

- Può lavorare con sensori di terze parti e opensource
- Può lavorare con scanner di terze parti/opensource oppure con i propri (NeWT, NEVO)
- Scanner rete/vulnerabilità separati
- Fortemente scalabile
- Complessità dell'installazione
- Scanning attivo
- Scanning passivo
  - OS fingerprinting
  - Daemon banner



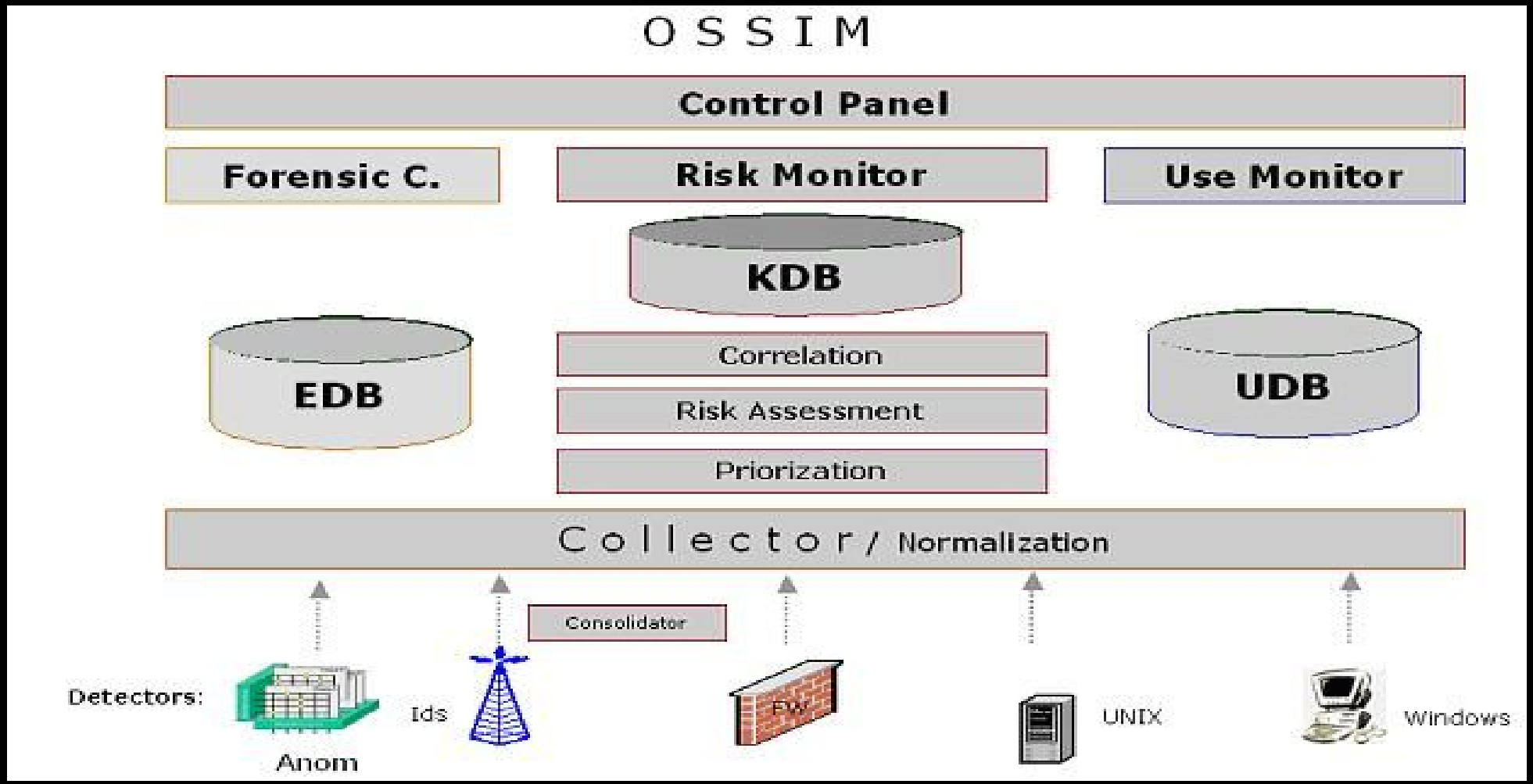
Improving detection: Security Information Management (SIM)

- Come gestire gli allarmi generati da tutti i dispositivi e i sistemi di sicurezza presenti in una grossa rete?

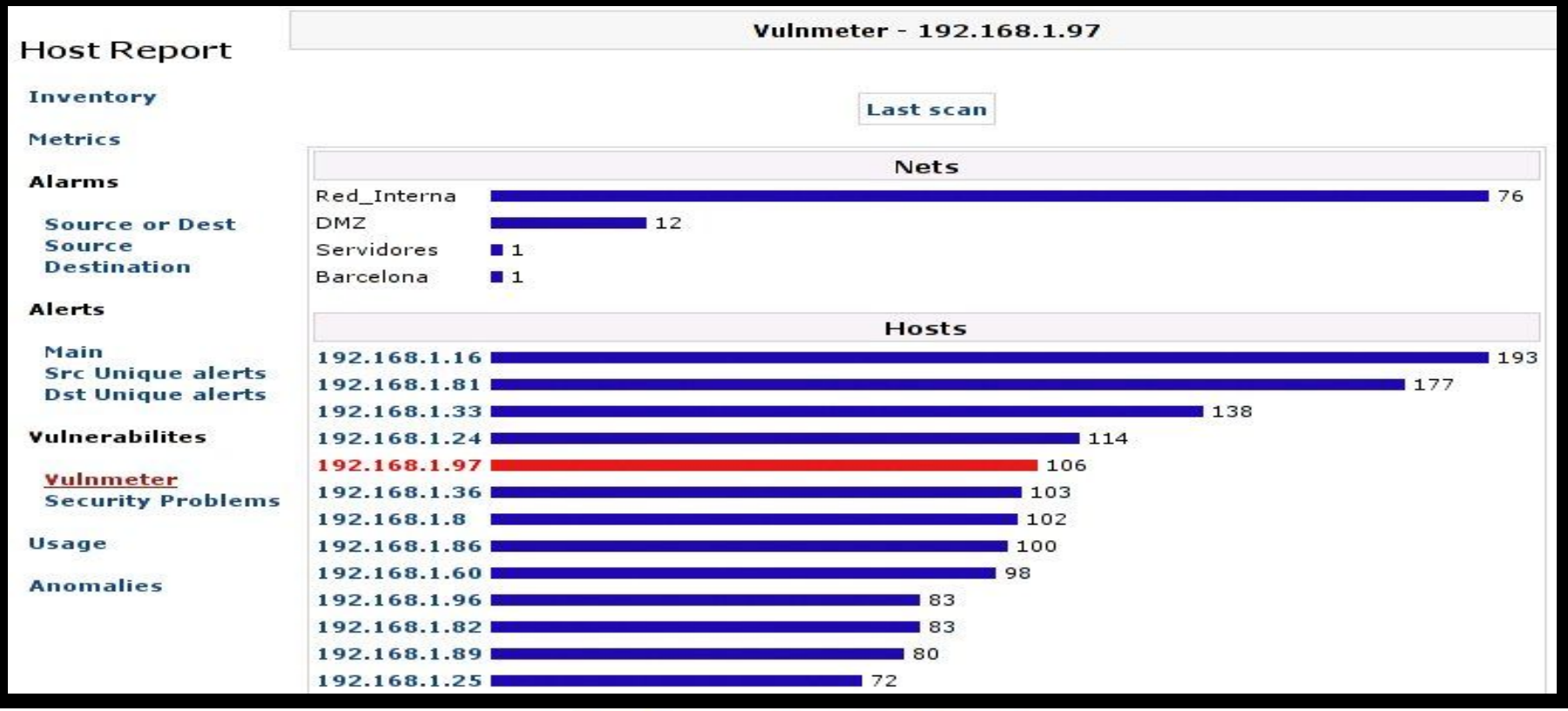
- I SIM permettono di automatizzare la raccolta di eventi gestendo:
  - normalizzazione e aggregazione: unificare tutti gli eventi secondo un formato comune definito (XML per esempio)
  - correlazione: gli eventi normalizzati sono classificati in funzione di asset (attività) o asset group a cui viene assegnato un punteggio di rischio globale
  - risk assessment: valutazione del rischio, calcolato in funzione di
    - incidenza dell'attacco
    - valore (di importanza) di un asset
    - vulnerabilità: probabilità che un attacco vada a buon fine su uno specifico asset
  - visualizzazione e reporting

L'architettura di OSSIM

- EDB: event database
- KDB: knowledge db
- UDB: user db, contiene il profilo di utilizzo dell'asset



Screen Shots OSSIM



<- Last 25 (650-675 of 1120) Next 25 ->

Alarm	Risk	Date	Source	Destination	Description	Delete
WEB cmd.exe access	4	2004-02-19 19:15:42	192.168.1.153:0	192.168.1.6:0	Forbidden and Not Found	Delete
WEB cmd.exe access	4	2004-02-19 19:15:42	192.168.1.153:0	192.168.1.6:0	Forbidden and Not Found	Delete
WEB cmd.exe access	5	2004-02-19 19:15:42	192.168.1.153:0	192.168.1.7:0	Forbidden and Not Found	Delete
WEB cmd.exe access	5	2004-02-19 19:15:42	192.168.1.153:0	192.168.1.7:0	Forbidden and Not Found	Delete
WEB cmd.exe access	4	2004-02-19 19:15:42	192.168.1.153:0	192.168.1.6:0	Forbidden and Not Found	Delete
WEB cmd.exe access	4	2004-02-19 19:15:42	192.168.1.153:0	192.168.1.6:0	Forbidden and Not Found	Delete
WEB cmd.exe access	5	2004-02-19 19:18:05	192.168.1.153:0	192.168.1.6:0	Attack-Response WEB cmd.exe access	Delete
WEB cmd.exe access	5	2004-02-19 19:18:05	192.168.1.153:0	192.168.1.6:0	Attack-Response WEB cmd.exe access	Delete
Successful DCOM exploit	10	2004-02-19 19:18:05	192.168.1.6:0	192.168.1.153:0	Windows cmd.exe attack response	Delete
WEB cmd.exe access	8	2004-02-19 19:18:05	192.168.1.6:0	192.168.1.153:0	Attack-Response WEB cmd.exe access	Delete
WEB cmd.exe access	5	2004-02-19 19:18:05	192.168.1.153:0	192.168.1.6:0	Attack-Response WEB cmd.exe access	Delete

Cisco Works: Architettura 3-Tier

Powerful and flexible 3-Tier architecture scales to any enterprise size

- All netForensics components are fully distributable from one server to many

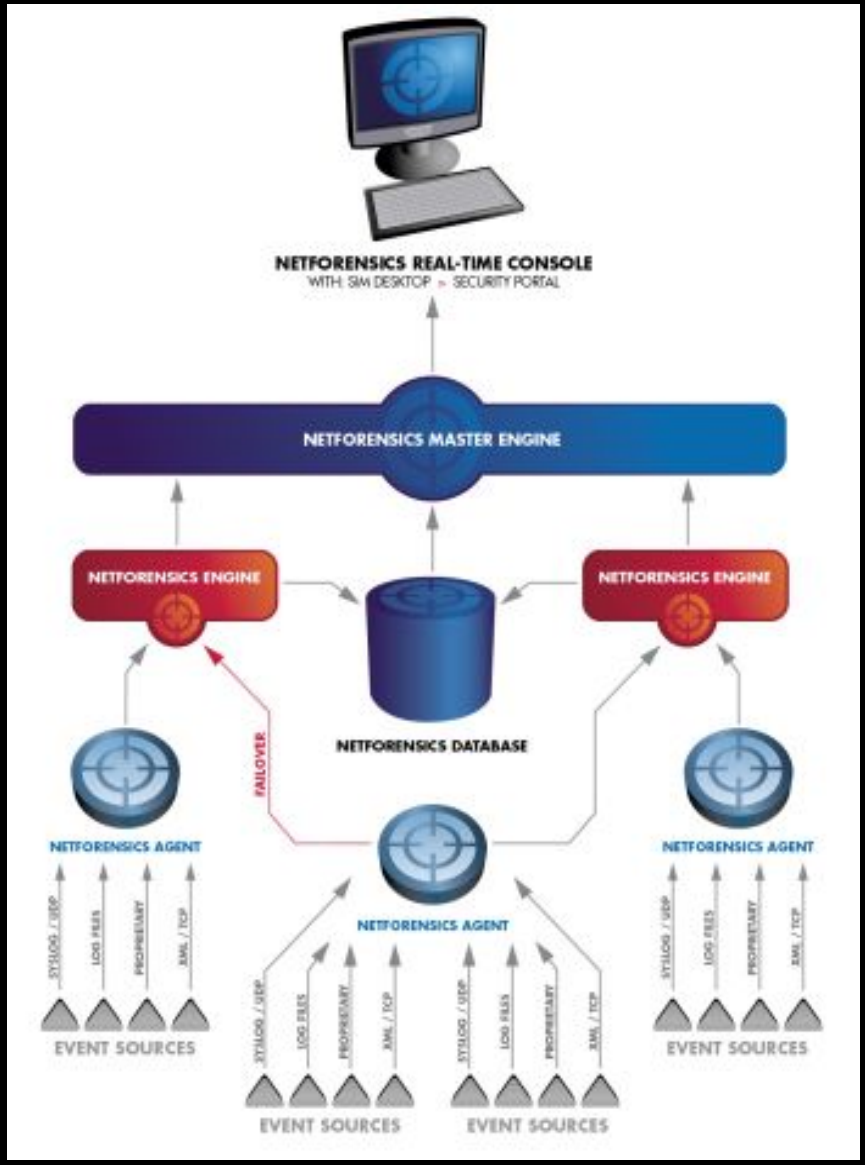
- Console for Centralized configuration, reporting & maintenance of software

- Agents Perform Event Collection & Normalization

- Engines Aggregate & Correlate Events

- Integrated database facilitates reporting, auditing & analysis

- Master Engine supports Visualization of Correlated Events



Dispositivi supportati: OSSIM VS Cisco Works

OSSIM

- Snort
- Nessun
- NTOP
- Snortcenter
- Acid
- Riskmeter
- Spade
- RRD
- Nmap
- P0f
- Arpwatch

Cisco Works

- Arbor peakflow DOS
- CheckPoint firewall 1
- Cisco IOS ACL, FW, IDS
- Cisco secure IDS, PIX
- Cisco VPN concentrator
- Cisco firewall switch module
- ISS HIDS e NIDS
- Sourcefire
- SNORT
- Solaris e Linux events
- Apache, IIS, iPlanet web server
- Windows 2000 events
- Symantec Enterprise FW/VPN

Dove ci stiamo muovendo?

- Affidabilità: livello di certezza garantito dall'IDS nell'identificazione degli eventi
  - Alta sensibilità=pochi falsi positivi
- Sensitività: capacità dell'IDS di rilevare anomalie e minacce
  - Alta sensitivtà=pochi falsi negativi

- Fine: diminuire sia il numero di falsi positivi che negativi
- Come:
  - valorizzando tutte le informazioni
  - modellando l'IDS in funzione del'asset
    - Router-IDS
  - utilizzando un IDS con architettura distribuita
  - garantendo livelli di dettaglio differenti

References

- Oltre a quelle citate nelle slide ricordo
  - Confronto tra tre diversi approcci target-based IDS: http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss306_ar540,00.html
  - Sourcefire technology: http://www.sourcefire.com/technology.html
  - Cisco Works: www.cisco.com/en/US/products/sw/cscowork/ps5209/index.html

- Un grazie particolare a Joel Snyder <Joel.Snyder@Opus1.COM> per le informazioni sui target-based IDS

- Questa presentazione sarà disponibile sul sito di S.P.I.N.E. http://www.spine-group.org